UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,471	10/11/2001	James L. Jason JR.	10559-504001 / P11796	9923

20985 7590 09/12/2007
FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DIVECHA, KAMAL B	
ART UNIT	PAPER NUMBER
2151	
MAIL DATE	DELIVERY MODE
09/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/976,471	JASON ET AL.	
	Examiner	Art Unit	
	KAMAL B. DIVECHA	2151	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-46 are pending in this application.

Claims 4-5, 8, 15-18, 22, 25-26, 33-34, 36, 38, 40, 42, 44-46 are cancelled.

Response to Arguments

Applicant's arguments filed June 29, 2007 with respect to claims above have been fully considered but are moot in view of the new ground(s) of rejection.

35 U.S.C. 112, first paragraph rejections

Applicant's arguments with respect to 35 U.S.C. 112, first paragraph rejections have been fully considered but are not persuasive for the reasons set forth below.

35 U.S.C. 101 rejection

Applicant's argument with respect to claim 35 U.S.C. 101 rejection have been fully considered but are not persuasive simply because the computer-readable medium is defined to include both the tangible and intangible medium such as transmission medium, wherein the intangible medium is incapable of producing "useful, concrete and tangible results". More specifically, such a transmission medium fails to structurally and functionally interconnect with the software in such a manner to, in and of itself, enable any usefulness to be realized.

Specification

The specification is objected to under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

The test to be applied under the written description portion of 35 U.S.C. § 112, first paragraph, is whether the disclosure of the application as originally filed reasonably conveys to the artisan that the inventor had possession at that time of later claimed subject matter. Vas-Cat, Inc. v. Mahurkar, 935 F. 2d 1555, 1565, 19 USPQ2d 111, 1118 (Fed. Cir. 1991), reh'rg denied (Fed. Cir. July 8, 1991) and reh'rg, en banc, denied (Fed. Cir. July 29, 1991).

The applicants have failed to provide an enabling disclosure in the detailed description of the embodiment. The specification is objected to under 35 U.S.C. § 112, first paragraph, as failing to support the subject matter set forth in these claims, i.e. lack of written description. See MPEP § 2163.

Independent claim 1 recites:

> A method comprising:
> first monitoring network traffic, and caching a 5-tuple packet information for request messages of a specified type;
> determining a number of valid and invalid request messages by analyzing the cached 5-tuple information cache;
> comparing current network traffic to the number of valid and invalid request messages, at first and second points of a network, and using said comparing to generate information about unwanted communications passing through the first and second points, the unwanted communications being of a type to reduce the ability of the target device to respond to other communications:
> communicating the information generated about the unwanted communications to brokers corresponding to the first and second points of the network;
> analyzing, by the brokers, the information generated about the unwanted communications; and
> communicating between the brokers to identify which of the points first carried the unwanted communications.

However, upon reviewing the originally filed specification, Examiner noted that there is no support and/or lacks a written description for the amendatory claim language and/or limitations in the original specification.

In other words, the originally filed specification fails to teach, disclose or suggest the process of determining a number of valid and invalid request messages by analyzing the cached 5-tuple packet information" and "comparing current network traffic to the number of valid and invalid request messages, at first and second points of a network..."

Applicant in response filed has cited the following portions of the specification for providing a written description of the subject matter in the claims:

> Contrary to the Office's assertion, the original specification reasonably conveys to a person having ordinary skill in the art that the applicants had possession of the claimed subject matter at the time of filing of the application. For example, the application as filed describes that request messages (e.g., SYN requests) in the network traffic can be monitored. (See, e.g., page 4, lines 19-23, which states that "[t]he sending communications monitor 42 **monitors** the messages, including the SYN requests, passing through the interface device 20 (step 502). The sending flood detector 46 detects that a flood is occurring through that interface device 20 (step 504).")
>
> Additionally, the application as filed describes that one example of SYN flood attack detection is by comparing the number of request messages with the network traffic, which includes a number of acknowledgment messages. (See, e.g., pages 6-7, which state that "In detecting a flood attack, a flood detector may employ one or more of several detection methods. For example, a flood detector can statistically analyze all communications through the interface device and determine that an uncharacteristically large number of SYN requests are passing through the interface device .... To detect an uncharacteristically large number of SYN requests, the **interface device can monitor the traffic through it to determine the normal level of traffic** .... Still another example of a flood detection method is **comparing or correlating the number of SYN requests with corresponding final ACK messages** in *order to* determine the number of SYN requests that are **valid or invalid.** A 5-tuple caching technique can be used to handle packets that have already been seen. When the first SYN message comes in, the cache won't have an entry for the 5-tuple of that message (source IP, destination IP, IP protocol, source port, and destination port). When subsequent packets arrive, there will already be cached information."

However, there is simply no indication, suggestion or disclosure in the cited portion of the original specification of the fact "determining a number of valid and invalid request messages by analyzing the cached 5-tuple information cache" and "comparing current network traffic to the number of valid and invalid request messages, at first and second points of a network..".

In fact, the specification discloses "Still another example of a flood detection method is **comparing or correlating the number of SYN requests with corresponding final ACK messages in order to determine the number of SYN requests that are valid or invalid**" (specification, pg. 7 lines 10-19).

First, it is clear from this passage that the process of determining a number of valid and invalid request messages **is not** achieved by analyzing the cached 5-tuple packet information, but is based on **comparing or correlating the number of SYN requests with corresponding final ACK messages.**

Secondly, the process of comparison is performed in order to determine the number of SYN requests that are valid or invalid, thus the process of comparing the current network traffic to the number of valid and invalid request messages remains unclear at least based on the specification.

As such, the above claimed limitations presents the subject matter situations and was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claims 1-3, 6-7, 9-14, 19-21, 23-24, 27-35, 37, 39, 41 and 43 are rejected under 35 U.S.C. 112, first paragraph, for the same reasons as set forth in specification above.

For examination purposes, the limitation "determining a number of valid and invalid messages..." will be interpreted as determining a ratio, i.e. a number, of the incoming to outgoing messages; and the process of "comparing current network traffic to the number of valid and invalid..." will be interpreted as comparing the current or incoming traffic with the historical data and/or information.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 1-3, 6-7, 9-14, 19-21, 23-24, 27-35, 37, 39, 41 and 43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites "5-tuple packet information" in the claim.

In the context of this claim, it is unclear what type of information the term is referring to.

Applicant is advised to clearly define the term in the context of the claims.

For examination purposes, the 5-tuple packet information will be interpreted as information related to communication and/or information related to a communication packet.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 31-35, 37, 39, 41 and 43 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 31 recites:

"A computer program embodied in a computer readable medium..."

First, based on the context of the claim, the claim fails to fall into any of the four enumerated categories of the statutory subject matter, as set forth above.

Secondly, the claim lacks an appropriate computer readable storage medium to define a structural and functional interrelationship between a computer program and other elements of a computer, which permit the functionality of the computer program and/or application to be realized.

The applicant specification is evidenced to disclose computer readable medium to include both tangible medium such as such as memory chips, magnetic media, optical media and intangible medium such as those delivered for execution electronically from a remote location, i.e. through transmission media.

The transmission media is incapable of producing useful, concrete (repeatable) and tangible results.

For the at least these reasons, the claim is considered non-statutory.

Claims 32-35, 37, 39, 41 and 43 are rejected for the same reasons as set forth in claim 31.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

4. Claims 1-3, 6-7, 9-14, 19-21, 23-24, 27-35, 37, 39, 41 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen et al. (hereinafter Chen, US 2002/0103916 A1) in view of Conklin et al. (hereinafter Conklin, US 5,991,881).

As per claim 1, Chen explicitly discloses a method comprising:

first monitoring network traffic, and caching a 5-tuple packet information (i.e. information such as source ip address, destination ip address, etc.) for request messages of a specified type (pg. 1 [0007-0008], pg. 2 [0027], pg. 3 [0035-0039], pg. 6 [0078-0079], fig. 6 item #32a, fig. 4 item #42, 44);

determining a number of valid and invalid request messages by analyzing cached 5-tuple packet information (pg. 3 [0035-0039], pg. 4 [0045-0048]: log of information including number

of packets seen by the data collector of certain type from a particular source, pg. 5 [0059-0061]: determining a ratio of incoming to outgoing packets which may include valid and invalid messages);

comparing current network traffic to a threshold, at first and second points of a network, and using said comparing to generate information about unwanted communications passing through the first and second points, the unwanted communications being of a type to reduce the ability of the target device to respond to other communications (pg. 1 [0006-0007], [0009], pg. 4 [0048-0052], pg. 5 [0059-0062], fig. 9 item #84, 86, 88, 89 and 90);

communicating the information generated about the unwanted communications to brokers corresponding to the first and second points of the network (pg. 4 [0045-0048]: communicating statistics or alert to the control center and/or data collector);

analyzing, by the brokers, the information generated about the unwanted communications (pg. 4 [0045-0048]);

communicating between the brokers to identify which of the points first carried the unwanted communications (fig. 4 item #46, 50, 52, fig. 6, fig. 9, pg. 2 [0027-0028], pg. 3 [0035-0038], pg. 4 [0045-0050]: communicating with control center and data collectors and gateways to identify and trace the source of the attack).

However, Chen does not disclose the process of comparing the current network traffic to the number of valid and invalid request messages, i.e. comparing the incoming traffic to a threshold or ratio obtained through monitoring.

Conklin, from the same field of endeavor discloses the process of comparing the incoming or current traffic with the historical data or information (col. 4 L45 to col. 5 L9, col. 7

L44-67: historical data may comprise the number of packets, type of packets, number of valid or invalid packets, source and destination addresses, etc.).

Therefore it would have been obvious to a person of ordinary skilled in the art at the time the invention was made to modify Chen in view of Conklin in order to compare the incoming traffic with the number of valid and invalid messages.

One of ordinary skilled in the art would have been motivated because it would have it would have identified an intrusion to a computer network and/or would have identified a reportable activity (Conklin: col. 7 L44-61).

As per claim 2, Chen discloses the process of detecting the direction of the unwanted communications (pg. 3 [0037]).

As per claim 3, Chen discloses the process of identifying the target device (pg. 3 [0037]).

As per claim 6, Chen discloses the process of correlating communications request messages with acknowledgement messages (pg. 1 [0006-0009], pg. 3 [0035], [0037]).

As per claim 7, Chen discloses the process of communicating information about the unwanted communications to brokers (pg. 1 [0007, 0009], pg. 2-3 [0031]).

As per claim 9, Chen discloses the process of blocking a portion of communications passing through the point through which the unwanted communications originated (pg. 2 [0028], pg. 2-3 [0031], pg. 4 [0043]).

As per claim 10, Chen discloses the process of blocking a portion of communication request messages passing through the point through which the unwanted communications originated (pg. 2-3 [0003], pg. 4 [0043], [0047]).

As per claim 11, Chen discloses the process wherein the target device comprises a web server (pg. 2 [0025], pg. 5 [0060], fig. 2-3).

As per claim 21, Chen discloses the system wherein the communications analyzer includes an interface monitor corresponding to each interface device and a communications link between the interface monitors (pg. 2-3 [0030-0031], fig. 1-3).

As per claim 27, Chen discloses the process in which the communications monitor also includes a statistics analyzer for statistically analyzing the messages passing through the plurality of agents (pg. 3 [0035], fig. 4 item #44, 50, fig. 6, fig. 9).

As per claim 35, Chen discloses the process wherein said network traffic of a specified type is a number of SYN requests (pg. 1 [0006-0011], fig. 4, fig. 10).

As per claims 12-14, 19-20, 23-24, 28-32, 37, 39, 41 and 43, they do not teach or further define over the limitations in claims 1-3, 6-7, 9-11, 21, 27 and 35. Therefore claims 12-14, 19-20, 23-24, 28-32, 37, 39, 41 and 43 are rejected for the same reasons as set forth in claims 1-3, 6-7, 9-11, 21, 27 and 35.

Additional References

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Sharp et al., US 2002/0131366 A1: Traffic Management Control.

b. Belissent, US 6,789,203 B1: Preventing DoS Attack.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAMAL B. DIVECHA whose telephone number is 571-272-5863. The examiner can normally be reached on Increased Flex Work Schedule.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Valencia Wallace can be reached on 571-272-3440. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kamal Divecha/

Kamal Divecha
Art Unit 2151
September 5, 2007.

VALENCIA MARTIN-WALLACE
PRIMARY EXAMINER